UNITED STATES BANKRUPTCY COURT
SOUTHERN DISTRICT OF NEW YORK

In re:

FRONTIER COMMUNICATIONS CORP., *et al*.,

Reorganized Debtors.

FOR PUBLICATION

Chapter 11

Case No. 20-22476 (MG)

MEMORANDUM OPINION ON SPOLIATION MOTION

A P P E A R A N C E S:

DAY PITNEY LLP
Counsel for Reorganized Debtors
One Stamford Plaza
263 Tresser Blvd., 7th Floor
Stamford, CT 06901
By: Stanley A. Twardy, Jr., Esq.

and

225 Asylum Street
Hartford, CT 06103
By: Elizabeth A. Alquist, Esq
Matthew J. Letten, Esq.
Caitlin M. Barrett, Esq.

and

195 Church Street, 15th Floor
New Haven, CT 06510
By: Jonathan B. Tropp, Esq.
Joshua W. Cohen, Esq.

CULPEPPER IP, LLC
Counsel for Movie Company Claimants
75-170 Hualalai Rd., STE B204
Kailua-Kona, HI 96740
By: Kerry S. Culpepper, Esq.

OPPENHEIM + ZEBRAK, LLP
Counsel for Record Company Claimants
4530 Wisconsin Ave., NW, Fifth Floor
Washington, DC 20016
By: Matthew J. Oppenheim, Esq.

MARTIN GLENN
CHIEF UNITED STATES BANKRUPTCY JUDGE

Pending before the Court is a motion ("Motion,"[1] ECF Doc. # 2464) by the Movie Company Claimants ("MCCs") seeking to impose sanctions on Frontier Communications Corp. ("Frontier") for alleged spoliation, pursuant to Federal Rule of Civil Procedure ("FRCP") 37(e). The MCCs also filed a supplemental brief. ("Supplemental Motion,"[2] ECF Doc. # 2467.) Frontier filed an opposition to the Motion ("Response,"[3] ECF Doc. # 2469), to which the MCCs

[1] The MCCs attach the following documents to their Motion: the Declaration of Kerry Culpepper ("Culpepper Decl."), the Declaration of Paul Garcia In Lieu of a Rule 30(b)(6) Deposition ("Garcia Decl."), Exhibit M-1 (email to Kerry Culpepper), Exhibit M-2 (Frontier's Responses to the Movie Company Claimants' Third Set of Requests for Admission), Exhibit M-3 (excerpts of two depositions of Philippe Levan: the date for one is unclear, the date for the other is November 12, 2024), Exhibit M-4 (Frontier internal emails), Exhibit M-5 (Frontier internal emails), Exhibit M-6 (Frontier internal emails), Exhibit M-7 (Frontier internal emails), Exhibit M-8 (Frontier internal email), Exhibit M-9 (emails between Culpepper and Frontier), Exhibit M-10 (MCCs' January 18, 2021 email to Frontier), Exhibit M-11 (emails between Culpepper and Frontier), Exhibit M-12 (emails between Culpepper and Frontier), Exhibit M-13 (emails between Culpepper and Frontier), Exhibit M-14 (Frontier internal emails), Exhibit M-15 (Frontier user declaration), Exhibit M-16 (code), Exhibit M-17 (code), Exhibit M-18 (excerpt of deposition of Jesse Ross ("Ross Dep.")), Exhibit M-19 (Reddit posts), Exhibit M-20 (notice), Exhibit M-21 (Frontier internal emails), Exhibit M-22 (MCCs' notice of 30(b)(6) deposition), Exhibit M-23 (excerpt of Kevin Vosburgh deposition), Exhibit M-24 (excerpt of Kevin Hartman deposition), Exhibit M-25 (Frontier's response to MCCs' Amended Second Set of Interrogatories).

[2] The MCCs attach Exhibit M-26 (Frontier's January 25, 2021 litigation hold memorandum) to this motion.

[3] Frontier attaches the following documents to their Response: the Declaration of Stanley A. Twardy, Jr., Exhibit 1 (excerpts from June 6, 2024 deposition of Philippe Levan ("June 6 Levan Dep.")), Exhibit 2 (excerpts of April 10, 2024 deposition of Philippe Levan ("April 10 Levan Dep.")), Exhibit 3 (excerpts of deposition of Joshua Elmore), Exhibit 4 (excerpts of deposition of Greg Hartman), Exhibit 5 (documents produced as FRONTIER_00179450 – 58), Exhibit 6 (FRONTIER_00179155 – 57), Exhibit 7 (FRONTIER_00179427 – 28), Exhibit 8 (document provided by Philippe Levan), Exhibit 9 (excerpts from deposition of Jesse Ross), Exhibit 10 (email from Frontier's counsel to Culpepper), Exhibit 11 (FRONTIER_00002307), Exhibit 12 (email from Frontier's counsel to Culpepper), Exhibit 13 (copy of subpoena sent by Culpepper to Frontier), Exhibit 14 (MOVIE724828 – 31), Exhibit 15 (excerpts from deposition of Alvin Mathew), Exhibit 16 (FRONTIER_00179479), Exhibit 17 (FRONTIER_00179426 – 29), Exhibit 18 (excerpts of deposition of John Greifzu), Exhibit 19 (excerpts of deposition of Albert Mauri), Exhibit 21 (MCCs' Second Request for Production of Documents Directed to Debtor), Exhibit 22 (FRONTIER_00178471), Exhibit 23 (excerpts of November 12, 2024 deposition of Philippe Levan ("Nov. 12 Levan Dep.")), the Declaration of Philippe Levan ("Levan Decl."), the Declaration of Greg Hartman ("Hartman Decl."), the Declaration of Albert Mauri ("Mauri Decl."), and the Declaration of Kevin Vosburgh ("Vosburgh Decl.").

filed a reply ("Reply,"[4] ECF Doc. # 2484). Evaluating the spoliation motion requires an understanding of the Digital Millenium Copyright Act, PUB. L. NO. 105-304 (1998) ("DMCA"), 15 U,S.C. §§ 101, *et seq.,* particularly the "safe harbor" affirmative defense the DMCA creates for an Internet service provider ("ISP") such as Frontier.[5] The MCC's spoliation motion asserts that Frontier destroyed digital evidence that the MCCs want to use to establish Frontier's secondary liability for copyright infringement, and also to defeat Frontier's safe harbor affirmative defense. Specifically, the MCCs challenge Frontier's loss of four or five sources of evidence[6]: (1) transcripts of customer calls; (2) the emails and documents of Greg Hartman, a former member of Frontier's "DMCA team"[7] who left Frontier in 2019; (3) system logs; and (4) accounting tables containing IP address assignment records from Frontier's RADIUS database.

The Record Company Claimants ("RCCs") and Frontier entered into a joint stipulation preserving the RCCs' right, in lieu of filing a motion pursuant to FRCP 37, to introduce evidence and argument at trial that "Frontier did not preserve certain Reports data, system logs, traceback files, and call transcripts, and . . . that the unavailability of this data has impacted the RCCs'

---

[4] The MCCs attach the following documents to their Reply: a second declaration by Kerry Culpepper, Exhibit M-27 (email from Frontier to Culpepper), Exhibit M-28 (excerpts from MCCs' rebuttal expert report by Stephen M. Bunting), Exhibit M-29 (FRONTIER_00029511), Exhibit M-30 (FRONTIER_00066408), Exhibit M-31 (FRONTIER_00066408), Exhibit M-32 (FRONTIER_00053500), Exhibit M-33 (FRONTIER_00178342), Exhibit M-34 (FRONTIER_00033698), Exhibit M-35 (complaint filed by nonparty Bodyguard Productions, Inc. against nonparty PacificDirect), Exhibit M-36 (email from Frontier's counsel to Culpepper), Exhibit M-37 (excerpts of April 10 Levan Dep.), Exhibit M-38 (excerpts of June 6 Levan Deposition), Exhibit M-39 (excerpts of Frontier's Second Supplemental Response to MCCs' RFAs), Exhibit M-40 (excerpts of Frontier's Third Supplemental Response to MCCs' RFAs), Exhibit M-41 (excerpts from the deposition of Albert Mauri), Exhibit M-42 (deposition of Paul Garcia).

[5] The DMCA is briefly discussed below. *See* Section I.C.

[6] Frontier lists five, including Reports tables (discussed below). It is unclear, but it may be that the MCCs confuse the RADIUS and DMCA databases (see Motion at 11); the MCCs appear to be primarily concerned with the deletion of the RADIUS data.

[7] The "DMCA team" is the name Frontier gave to the group of employees that meets at least quarterly to review information about subscriber accounts and to decide whether to terminate Internet service to any subscribers. (Response at 4.)

analysis and presentation of evidence." (ECF Doc. # 2461 at 1.) Frontier, in turn, reserved the right to introduce evidence and argument in response. (*Id.* at 2.)

Because the Court does not have sufficient evidence to determine either the extent of the prejudice to the plaintiffs or the mental state of Frontier's employees that deleted relevant data, the Court withholds ruling on the majority of the MCCs' Motion at this time. With two exceptions: the Court **DENIES** the MCCs' Motion to the extent it seeks spoliation sanctions for the deletion of Greg Hartman's emails and the Records tables. The Court finds, for reasons discussed below, that Frontier had no obligation to preserve Hartman's emails at the time of their destruction, and that Frontier preserved all Records tables which it was obligated to keep. With respect to the RADIUS database entries, the system log text files, and the call transcripts, for now the Court **DENIES WITHOUT PREJUDICE** the MCCs' Motion but will permit the MCCs to join with the RCCs in presenting evidence of Frontier's failure to preserve this evidence and argue at trial for spoliation sanctions. Frontier will likewise be permitted to defend the spoliation motion.

I. BACKGROUND

A. Plaintiffs' Case in Chief

The MCCs and RCCs have filed claims against Frontier alleging secondary copyright infringement liability. The standards for liability are largely set out in an earlier opinion in this case, *In re Frontier Communications Corp.*, 658 B.R. 277, 288–95 (Bankr. S.D.N.Y. 2024), and are briefly recapitulated here.

To prove secondary copyright liability of an ISP, the plaintiffs must first prove direct copyright infringement by an ISP's subscriber. *See BMG Rts. Mgmt. (US) LLC v. Cox Commc'ns, Inc*., 149 F. Supp. 3d 634, 663 (E.D. Va. 2015) ("*Cox I*") , *aff'd in part, rev'd in part*,

881 F.3d 293 (4th Cir. 2018) ("*Cox II*") ("BMG cannot hold Cox liable for contributory or vicarious infringement absent evidence of underlying direct infringement."); *After II Movie, LLC v. Grande Commc'ns Networks, LLC*, No. 1:21-CV-709-RP, 2023 WL 1422808, at *3 (W.D. Tex. Jan. 31, 2023), *report and recommendation adopted*, No. 1:21-CV-709-RP, 2023 WL 2671399 (W.D. Tex. Mar. 28, 2023) ("There cannot be secondary infringement without direct infringement."). As discussed further below, the RADIUS database allows Frontier to identify its subscribers' names with the IP addresses assigned to them by Frontier at the date and time of the alleged infringement included in DMCA notices sent to Frontier by copyright holders alleging that their protected works were infringed by Frontier's subscribers. Whether Frontier's deletion of RADIUS data prejudiced the plaintiffs, and if so, to what extent, rests in part on the question whether the plaintiffs have sufficient evidence to prove direct infringement without the RADIUS data. Without the benefit of full briefing on this question, the Court briefly addresses prior caselaw on proving contributory infringement by an ISP, without the necessity of proving direct infringement by identified subscribers. In other secondary liability cases against ISPs premised on a large number (hundreds or thousands) of instances of direct copyright infringement by subscribers, plaintiffs were not required to litigate every individual instance of direct infringement to prove the ISP's liability. *See, e.g.*, *Cox I*, 149 F. Supp. 3d at 663–64 ("[I]mposing a rule that would require copyright owners to litigate John Doe [direct infringement] lawsuits before bringing claims of secondary liability would undermine a key purpose of secondary liability claims . . . . . 'When a widely shared service or product is used to commit infringement, it may be impossible to enforce rights in the protected work effectively against all direct infringers, the only practical alternative being to go against the distributor of the copying device for secondary liability on a theory of contributory or vicarious liability.'" (citing

MGM Studios, Inc. v. Grokster, 545 U.S. 913 at 929–30 (2005))). It appears that plaintiffs can instead use circumstantial evidence to establish direct infringement if that evidence gives rise to an inference that subscribers used the defendant ISP's service to directly infringe. *See id.* ("[Plaintiff] may establish direct infringement using circumstantial evidence that gives rise to an inference that [defendant's] account holders or other authorized users accessed its service to directly infringe . . . . While identity [of individual subscribers] is a key issue in many individual infringement suits, it has little relevance in a large-scale secondary liability suit."); *see also Capitol Recs., Inc. v. Thomas*, 579 F.Supp.2d 1210, 1225 (D. Minn. 2008) ("[D]irect proof of actual dissemination is not required by the Copyright Act. Plaintiffs are free to employ circumstantial evidence to attempt to prove [a violation]."); *After II Movie, LLC*, 2023 WL 1422808, at *2–3 (holding that, where plaintiff sought to impose contributory liability upon an ISP and not direct liability upon an individual subscriber, identifying alleged direct infringers by IP address only was sufficient to move past motion to dismiss); *Bodyguard Productions, Inc. v. RCN Telecom Services, LLC*, No. 3:21-CV-15310-GCTJB, 2022 WL 6750322, at *5–6 (D.N.J. Oct. 11, 2022) (holding that plaintiff adequately pleaded secondary copyright infringement and could progress past motion to dismiss when it alleged infringement at defendant-owned IP addresses, but not by specific subscribers). Regardless, the MCCs in this case have indicated that they wish to prove direct infringement by showing that at least a subset of Frontier subscribers, whose IP addresses were flagged for infringement, actually infringed on the MCCs' copyrights. *See In re Frontier Communications Corp.*, 655 B.R. 413, 418 (Bankr. S.D.N.Y. Dec. 1, 2023). This caselaw raises the question whether the MCCs and RCCs have suffered sufficient prejudice as a result of Frontier's deletion of information from the RADIUS database. This remains an open question for trial.

Secondary liability can be broken down into contributory and vicarious liability. Under the "contributory" umbrella, there exists liability both for (1) *inducement* as well as (2) *material contribution*, both carrying a knowledge requirement. Specifically, "one who, with knowledge of the infringing activity, induces, causes or materially contribute*s* to the infringing conduct of another, may be held liable as a 'contributory' infringer.'" *Gershwin Publ'g Corp. v. Columbia Artists Mgmt., Inc*., 443 F.2d 1159, 1162 (2d Cir. 1971) ("*Gershwin*"). Once knowledge of direct infringement is established, either prong—inducement or material contribution—is sufficient to establish liability. *See Faulkner v. Nat'l Geographic Soc'y*, 211 F. Supp. 2d 450, 473 (S.D.N.Y. 2002), *aff'd*, 409 F.3d 26 (2d Cir. 2005) ("*Faulkner*"). The knowledge standard is an objective one, imposing liability on persons who "know or have reason to know" of the direct infringement. *Arista Recs., LLC v. Doe 3*, 604 F.3d 110, 118 (2d Cir. 2010) (quoting *A&M Recs., Inc. v. Napster, Inc.*, 239 F.3d 1004, 1020 (9th Cir. 2001), *aff'd*, 284 F.3d 1091 (9th Cir. 2002) ("*Napster*")). The standard is thus met if one has constructive knowledge but remains willfully blind. *Cox II*, 881 F.3d at 308. In the context of ISP liability for copyright infringement, ISPs have sufficient knowledge when they have enough information to "*do* something about [the infringement]." *Id.* at 312 (emphasis in original). With knowledge established, a plaintiff can either state a claim for inducement, which "premises liability on purposeful, culpable expression and conduct" and requires "active steps taken to encourage direct infringement," *Grokster*, 545 U.S. at 915; or for material contribution "to the infringing conduct of another," *Doe 3*, 604 F.3d at 117 (quoting *Gershwin*, 443 F.2d at 1162). The "classic instance of inducement" is "advertisement or solicitation that broadcasts a message designed to stimulate others to commit violations," such that "[t]he unlawful objective is unmistakable." *Grokster*, 545 U.S. at 916. As for material contribution, it must be more than "a mere

quantitative contribution to the primary infringement: in other words, the participation or contribution must be substantial." *Arista Recs. LLC v. Usenet*, 633 F. Supp. 2d 124, 155 (S.D.N.Y. 2009) (quoting *Faulkner,* 211 F. Supp. 2d at 473 (internal quotation marks and citation omitted)). In the online space, "substantial contribution is found where an internet service provider's servers 'are the sole instrumentality of their subscribers' infringement.'" *Capitol Recs., Inc. v. MP3tunes, LLC*, 821 F. Supp. 2d 627, 648 (S.D.N.Y. 2011) (quoting *Usenet*, 633 F. Supp. 2d at 155). An ISP that continues to provide that crucial conduit despite knowledge of infringing activity satisfies this standard. *Sony Music Ent. v. Cox Commc'ns, Inc*., 93 F.4th 222, 236 (4th Cir. 2024) ("*Cox V*") ("[S]upplying a product with knowledge that the recipient will use it to infringe copyrights is exactly the sort of culpable conduct sufficient for contributory infringement.")

Vicarious liability, by contrast, imposes liability (regardless of knowledge) when one has both (1) *supervision or control* over, and (2) a *direct financial interest* in, the infringing activity. *Gershwin*, 443 F.2d at 1162. Both elements are necessary; the "failure to satisfy either element is fatal to a claim for vicarious infringement." *Totally Her Media, LLC v. BWP Media USA, Inc.*, No. CV 13-08379-AB (PLAx), 2015 WL 12659912, at *7 (C.D. Cal. Mar. 24, 2015). As for supervision or control, "[t]he ability to block infringers' access to a particular environment for any reason whatsoever is evidence of the right and ability to supervise," *Usenet*, 633 F. Supp. 2d at 157 (internal citation omitted); if a defendant has the *right* to block access, such right must be "exercised to its fullest extent" to "escape imposition of vicarious liability," *Napster*, 239 F.3d at 1023. In the ISP context, courts have found that the ability to terminate or block its subscribers' accounts satisfies this prong. *See In re Frontier Communications*, 658 B.R. at 293 (collecting cases). The second prong of the vicarious liability inquiry requires "an obvious and direct

financial interest in the exploitation of copyrighted materials," *Shapiro, Bernstein & Co. v. H. L. Green Co.*, 316 F.2d 304, 307 (2d Cir. 1963); this can look like an ISP hosting infringing material as a "draw" to attract subscribers, *see, e.g.*, *Napster*, 239 F.3d at 1023, so long as "a causal relationship exists between the infringing activity and a financial benefit to the defendant. If copyright infringement draws customers to the defendant's service or incentivizes them to pay more for their service, that financial benefit may be profit from infringement. But in every case, the financial benefit to the defendant must flow directly from the third party's acts of infringement to establish vicarious liability," *Cox V*, 93 F.4th at 231–32 (internal citations omitted).

The burden of proving secondary liability rests squarely on the shoulders of the plaintiffs. *See Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1113 (9th Cir. 2007) ("The DMCA notification procedures place the burden of policing copyright infringement—identifying the potentially infringing material and adequately documenting infringement—squarely on the owners of the copyright. We decline to shift a substantial burden from the copyright owner to the [service] provider."); *Wolk v. Kodak Imaging Network, Inc*., No. 10 CIV. 4135 RWS, 2011 WL 940056, at *5–9 (S.D.N.Y. Mar. 17, 2011) (adopting the holding in *CCBill*: "The DMCA is explicit: it shall not be construed to condition 'safe harbor' protection on a service provider monitoring its service or affirmatively seeking facts indicating infringing activity . . . . [T]he DMCA . . . places the burden of uncovering infringing activity on copyright holders.") (internal citation omitted).

Here, of course, evidence linking IP addresses included in DMCA notices with the names of the subscribers who allegedly infringed the claimants' copyrights is exclusively in Frontier's possession. To the extent Frontier deleted that information, it is unavailable to the plaintiffs.

That circumstance raises an important issue: what evidence must the MCCs and RCCs prove to establish their claims. The caselaw briefly discussed above may enable the MCCs and RCCs to prove their claims without the information contained in the RADIUS database that Frontier has destroyed. This is relevant to the issue of prejudice, central to imposition of remedies for spoliation. Further briefing and the evidence at trial will be needed to resolve these questions.

Assuming the information in the RADIUS database should have been retained, consideration of the spoliation motion raises the issue of the time period during which that information should have been retained. The applicable statute of limitations bears directly on that issue and is addressed in the next section of this Opinion.

B. Statute of Limitations

The statute of limitations for copyright infringement is governed by 17 U.S.C. § 507(b), which provides in relevant part: "No civil action shall be maintained under the provisions of this title unless it is commenced within three years after the claim accrued." This Court previously determined that, since Frontier filed for bankruptcy on April 14, 2020, and section 108(c) of the Bankruptcy Code has the effect of extending back the statute of limitations for claims against Frontier filed by the bar date for three years from the day "before filing of the petition," the claimants could bring copyright claims based on actions dating back to April 13, 2017.[8] *See In re Frontier Communications Corp.*, 655 B.R. at 420–21. Whether an earlier date should be applied in considering Frontier's DMCA section 512 affirmative defense is an issue for another day. The focus of this Opinion so far has been the discovery and evidence the MCCs and RCCs may need to make out their *prima facie* case. But to prepare their cases for trial, the claimants

[8] The Court also held that the MCCs could seek discovery—specifically, identifying information for Frontier subscribers which the MCCs have reason to believe infringed on their copyrights—dating back to October 14, 2016, six months before the statute of limitations expired. *Id.* at 421. For purposes of the spoliation motion, the Court limits its focus to the period covered by the statute of limitations.

were entitled to discovery of relevant evidence to rebut Frontier's assertion of a safe harbor affirmative defense. The Court addresses that issue now, without foreclosing other arguments that the parties may make at trial.

C. Frontier's Anticipated Defense

Frontier denies liability and anticipates asserting defenses under section 512 of the DMCA. 17 U.S.C. 512. In short, the DMCA is a federal statute which updates copyright law to address issues created by the Internet and the use of new technology. One of its core aims is to establish protections for online service providers if their users engage in copyright infringement, including by creating a notice-and-takedown system enabling copyright owners to inform service providers about infringing material so that the provider can take it down. It also provides certain safe harbors for, among others, ISPs. As this Court previously pointed out, these DMCA safe harbors are affirmative defenses for which Frontier bears the burden of proof. *In re Frontier Commc'ns Corp*., 658 B.R. at 302 n.13 ("[I]nvocation of the DMCA is an affirmative defense that requires additional factual inquiry."); *see also BWP Media USA Inc. v. Polyvore, Inc*., 922 F.3d 42, 54–55 (2d Cir. 2019) ("Since the DMCA safe harbors are affirmative defenses, a defendant generally has the initial burden of establishing that it meets the statutory requirements.").

Frontier asserts a safe harbor defense under section 512 of the DMCA, as discussed further below. Frontier bears the burden of proof in establishing each of the elements of the affirmative defense. How Frontier will do so without the information contained in the RADIUS database remains an issue for trial and not for decision in this opinion dealing with the MCCs' spoliation motion.

The DMCA safe harbors "provide protection from liability for: (1) transitory digital network communications; (2) system caching; (3) information residing on systems or networks at the direction of users; and (4) information location tools." *Ellison v. Robertson*, 357 F. 3d 1072, 1077 (9th Cir. 2004) (citations omitted). These correspond with sections 512(a), 512(b), 512(c), and 512(d) of the DMCA. To take advantage of *any* of the safe harbors, a defendant must first show that it meets the conditions set forth in section 512(i):

> (i) Conditions for Eligibility.
>
> (1) Accommodation of technology. The limitations on liability established by this section shall apply to a service provider only if the service provider—
>
> > (A) has adopted and reasonably implemented, and informs subscribers and account holders of the service provider's system or network of, a policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or network who are repeat infringers; and
> >
> > (B) accommodates and does not interfere with standard technical measures.

17 U.S.C. § 512(i).

To fulfill the requirements of section 512(i), "a service provider must (i) adopt a policy that provides for the termination of service access for repeat infringers; (ii) inform users of the service policy; and (iii) implement the policy in a reasonable manner." *Wolk v. Kodak Imaging Network*, 840 F. Supp.2d 724, 744 (S.D.N.Y. 2012). "[T]he threshold requirement of the adoption of a repeat infringer policy should not be an overly burdensome one to meet," and courts in this district have found a service provider's implementation sufficient when it "demonstrate[d] that it took a clear position that those who chose to violate another's copyright would not be permitted to avail themselves of the service . . . provide[d]." *Capitol Recs., LLC v. Vimeo, LLC*, 972 F. Supp. 2d 500, 513 (S.D.N.Y.), *amended on reconsideration in part*, 972 F. Supp. 2d 537 (S.D.N.Y. 2013), *and aff'd in part, vacated in part, remanded*, 826 F.3d 78 (2d Cir.

2016). As for the second requirement of informing users of the policy, this requires "that the service provider put users on notice that they face exclusion from the service if they repeatedly violate copyright laws." *Id.* (cleaned up). Finally, while the "reasonable implementation" prong does not require that the service provider "affirmatively police its users for evidence of repeat infringement," a "substantial failure to record [infringers]" may "raise a genuine issue of material fact as to the implementation of the service provider's repeat infringer policy." *Perfect 10, Inc.*, 488 F.3d at 1109–11; *see also Ellison*, 357 F.3d at 1080 (finding that defendant had not reasonably implemented a repeat infringer policy where it "allowed notices of potential copyright infringement to fall into a vacuum and to go unheeded"); *In re Aimster Copyright Litig*., 334 F.3d 643, 655 (7th Cir.2003) (holding that policy was not reasonably implemented because, "by teaching its users how to encrypt their unlawful distribution of copyrighted materials [defendant] disable[d] itself from doing anything to prevent infringement"). Implementation also has been deemed unreasonable when service providers failed to terminate users who "repeatedly or blatantly infringe copyright." *Perfect 10, Inc.*, 488 F.3d at 1109; *see also Datatech Enters. LLC v. FF Magnat Ltd.*, No. C 12–04500(CRB), 2013 WL 1007360, at *6 (N.D.Cal. Mar. 13, 2013) (finding a policy "woefully inadequate" when the evidence "show[ed] that when [defendant] learned that particular users were engaged in extensive repeat infringement . . . [defendant] regularly declined to ban them despite requests from copyright holders"). "Implementation . . . need not be perfect. Rather, by the terms of the statute, it need only be 'reasonable.'" *Vimeo*, 972 F. Supp. 2d at 515. However, also per the terms of the statute, the repeat infringer policy must provide for the (eventual) termination of repeat infringers. *See Cox I*, 149 F. Supp. 3d at 658 ("To implement the repeat infringer policy contemplated by § 512(i), the penalty imposed by service providers must be termination.").

The focus here on the spoliation Motion is the evidence that has been destroyed that is needed either to advance the defense or rebut it. A plaintiff (here the claimants) facing an ISP mounting a section 512(i) argument can attack this affirmative defense by challenging the existence of a repeat infringer policy; or by showing that the service provider did not inform its subscribers of the policy, failed to implement the policy in question in a reasonable manner, or failed to accommodate (or interfered with) standard technical measures (technology used by copyright owners to identify or protect copyrighted works, *see Wolk v. Kodak Imaging Network, Inc.*, 840 F. Supp. 2d 724, 744–45 (S.D.N.Y. 2012), a*ff'd sub nom. Wolk v. Photobucket.com, Inc*., 569 F. App'x 51 (2d Cir. 2014)). If Frontier, as the MCCs allege, destroyed evidence pertaining to its repeat infringer policy (for example, pertaining to its application, implementation, or efficacy), whether Frontier can carry its burden to establish the affirmative defense without the evidence it deleted from the RADIUS database remains to be seen. It is not the issue for today. But the MCCs and RCCs are entitled to discovery to build their case to rebut any case presented by Frontier supporting the safe harbor defense.

D. Spoliation Motion

An overview of Frontier's copyright infringement-tracking technology is in order.

1. Frontier's Recordkeeping Technology

Since at least 2012, copyright holders have been sending email notices ("Notices") to Frontier alleging that IP addresses assigned to Frontier's subscribers are being used for copyright infringement. (ECF Doc. # 2460 ("Joint Stipulation of Facts" or "Joint Stip.") ¶ 1.) A Notice typically lists a copyrighted work, an IP address, and a time stamp at which the IP address was allegedly being used to share the work. (*Id.* ¶ 8.) To process incoming Notices, Frontier uses a computer script ("dmca-xml.py," or the "DMCA script"), which tries to identify the subscriber

account assigned to the IP address specified in the Notice when the alleged infringement occurred. (Response at 2.) To do this, the DMCA script uses another computer script ("radsearch") to query Frontier's IP address assignment data (including the RADIUS database, discussed below). (*Id.* at 3.)

a. RADIUS Database

Frontier maintains a database called the Remote Authentication Dial-in User Service ("RADIUS") database, which contains records of which IP address was assigned to a given customer at a particular time. (Levan Decl. ¶ 20; June 6 Levan Dep. Tr. 223:19–24 (explaining that the role of the RADIUS database is to keep track of changes to subscribers' IP addresses).) The RADIUS database allows Frontier to determine which cable modem or gateway relates to which IP address at a given time. (Joint Stip. ¶ 4.) By matching both an IP address and a subscriber identity to a cable modem or gateway, the RADIUS database allows Frontier to match subscribers to specific IP addresses at a specific date and time. (*Id.*) This does not work for all subscribers, since Frontier never maintained a record in the RADIUS database for every single subscriber. (*Id.*) Frontier also explains that one cannot always match an IP address with a subscriber at a given time because "sometimes no subscriber was assigned the IP address at the time alleged, or the IP address assignment is unreliable." (Response at 3.) Sometimes, a radsearch query only returns a MAC address or a BRAS interface (an identifier for a network router nearest the subscriber's location). (*Id*.) If a radsearch query (attempting to identify the subscriber associated with an IP address at which copyright infringement allegedly occurred) failed to turn up an IP address assignment information at the time specified in the Notice at issue—i.e., if the RADIUS database did not include the relevant IP address assignment information—the automated process would be "exhausted" and the subscriber would not be

notified of the alleged infringement (see below for an explanation of the notification system). (June 6 Levan Dep. Tr. 97:17–98:13.) Similarly, for most but not all subscribers, the RADIUS database contains "histories of dynamic IP addresses assigned to those subscribers." (Joint Stip. ¶ 15.) (The RADIUS database records new IP address assignments as they are made in a "current" accounting table, which is periodically saved, formerly each month, now each week. (Levan Decl. ¶ 21.)) This is relevant because there is no one-to-one relationship between IP addresses and subscribers: one subscriber can have numerous IP addresses over time, so to identify a particular user associated with it, one would have to know which subscriber was assigned that IP address during a specific time period. (*See* Exhibit M-21 to the Motion (February 4, 2020 email from Philippe Levan to John Greifzu: "That IP address is in a dynamically-assigned pool, which means that we would need a specific time period to identify the customer without ambiguity."); *see also* June 6 Levan Dep. Tr. 223:19–224:9.)

Until January 2024, Frontier purged IP address assignment records two years old or older from the RADIUS database. (Motion at 8.) Philippe Levan, a member of Frontier's DMCA team, testified that preserving the RADIUS database did not occur to him when he received the litigation hold memorandum in January of 2021, since he viewed Frontier's DMCA database (described below) as the "database of record with respect to the IP addresses associated with allegedly infringing activity." (Levan Decl. ¶ 24.) In January 2024, Frontier shortened the length of time it allowed IP address assignment records to remain in the database from 24 months to 18 months; according to Frontier, this was due to space constraints on the RADIUS server.[9] (Motion at 10–11; Levan Decl. ¶ 32.) At two different points in time, Frontier

[9] According to Philippe Levan, this is because Frontier "started receiving from the network more updates than we were previously getting," and Frontier's server was no longer able to sustain two years' worth of records: "while previously we may have been able to keep two years on the server we had to—we're currently able to keep only 18 months." (June 6 Levan Dep. Tr. 226:9–19.)

endeavored to preserve historical IP address assignment records. In March 2021, Levan directed his colleague to preserve old accounting tables for use in this litigation.[10] (Levan Decl. ¶ 28.) The colleague saved three months of historical accounting tables at that time, and then "[s]everal months later, [he] saved another three months of historical accounting tables from the RADIUS database," meaning that data from January through June 2019 was saved. (*Id.* ¶ 29, 36.) Levan's directive was subsequently forgotten, per Frontier, and preservation efforts ceased; Levan also forgot, for a time, that his colleague had preserved these tables. (*Id.* ¶¶ 30–31.) Frontier continued to purge IP address assignment records from the RADIUS database through document discovery in this case, though Levan started to archive historical records after his deposition in June 2024. (*Id*. ¶ 34.)

b. DMCA Database

Once Frontier receives a Notice, it sometimes takes additional action. Frontier maintains a database (the "Frontier DMCA Database") to track the actions it took to respond to the Notices. (Joint Stip. ¶ 3.) The Frontier DMCA database is comprised of three tables, labeled Reports, Notifications, and WG_Intercept. (*Id.*) This data is pulled, in part, from the RADIUS database (via the operation of the radsearch script, as discussed above).

The Reports table contains "records of Notices that Frontier has received, parsed, and processed" "successfully." (*Id.* ¶¶ 3, 5.) (The parties do not define "success.") Records in the table (each record a "Report"), created by the DMCA script, identify the subscriber account associated with a particular processed Notice, "to the extent Frontier's DMCA script identified the subscriber from the RADIUS database" (as discussed, this ability is limited, so the data in the Reports table is similarly limited, and therefore the Reports table cannot be used to definitively

[10] This request is reflected in Exhibit 7 to the Response.

identify the subscriber account associated with every Notice or IP address at a given time). (*Id.* ¶¶ 5, 10.) Each Report includes some identifying information for the subscriber whose account was associated with the IP address in the originating Notice at the date and time of alleged infringement specified in the Notice—whatever information associated with that address at that exact time is available in the RADIUS database. (*Id.* ¶ 8.) Such identifying information can include the subscriber's username, e-mail address, or MAC address. (*Id.*) Each individual Report reflects the IP address assignment at the date and time specified in the corresponding Notice, but not at other times. (*Id.* ¶ 9.) If the IP address in a Notice is not assigned to a particular subscriber at the time of infringement alleged in the Notice, or if the IP address assignment in Frontier's systems has not been refreshed within a specified time period, Frontier's DMCA script does not create a Report. (*Id.* ¶ 10.) Prior to March 2, 2020, the retention period for the Reports table was six months—a computer script would automatically delete records older than six months on a daily basis. (*Id.* ¶ 6; Levan Decl. ¶ 5.) Between March 2, 2020, and January 15, 2021, the retention period was 12 months.[11] (Joint Stip. ¶ 6.) The parties stipulated that, on January 15, 2021, the retention period was extended indefinitely. (*Id*.) However, Philippe Levan avers that he extended the retention period by disabling the daily deletion computer script on *January 25*, upon receipt of a litigation hold provided by Frontier's in-house counsel, Paul Garcia. (Levan Decl. ¶¶ 7–10.) The parties stipulated that the Reports table stores reports of Notices "successfully processed by Frontier from September 2, 2019 onward." (Joint Stip. ¶ 7.)

[11] According to Levan, every retention period was set, and every decision to change the retention period was implemented, upon the recommendation of Frontier's counsel. (Nov. 12 Levan Dep. Tr. at 368:1–372:19; Levan Decl. ¶ 6.)

According to Levan, the Reports table, as produced to the plaintiffs, contains "over 58,000 entries for Notices received by Frontier since September 2, 2019 concerning the MCCs' works, corresponding to over 15,000 unique subscriber accounts, of which over 11,000 are identified by name." (Levan Decl. ¶ 14(a).)

The Notifications table contains records of emails ("Notifications") which Frontier tried to send to subscribers whose IP addresses were associated with Notices. (Joint Stip. ¶ 3.) A subscriber's IP address would have to be associated with a certain threshold number of Notices before Frontier would take action. Before March 11, 2021, that threshold number was 16 Notices linked to an IP address assigned to a particular subscriber within 90 days; on March 11, 2021, Frontier changed the threshold to 11 notices within 90 days, and on May 9, 2021, Frontier revised its threshold again to 11 notices within three years. (*Id.* ¶ 13, 14.) Paul Garcia, Frontier's in-house counsel, testified that "[i]n most cases, it is not possible to determine a complete IP address assignment history from Notification records." (Garcia Decl. at 5.)

According to Levan, the Notifications table contains "over 40,000 entries during the period up to September 1, 2019 for Notifications sent to subscribers whose accounts were assigned an IP address that was the subject of a Notice concerning one of the MCCs' asserted works. These Notifications were sent to over 2,300 unique subscriber accounts." (Levan Decl. ¶ 14(b).) Together, the Reports and Notifications tables "identify over 17,000 unique subscriber accounts that were the subject of MCC Notices [Notices sent by MCCs], and for over 1,300 of these accounts, the Notifications table identifies the subscriber's 'preferred' email address (*i.e.*, email addresses provided to Frontier as their preferred contact." (*Id.* ¶ 14(c).)

The WG_Intercept table contains records of "Walled Garden intercepts" which Frontier tried to use on users of IP addresses assigned to accounts that were subject to a certain number of

notices (initially 100 Notices over 90 days, now 30 Notices over three years). (Response at 3.) This "intercept" directs the user subject to this threshold number of Notices to a webpage requiring acknowledgment of Frontier's Acceptable Use Policy before browsing the Internet. (*Id.*) The WG_Intercept table is created by a computer script contemporaneously with (1) the processing of a Notice; (2) an attempt to email a Notification; or (3) initiation, acknowledgment, or removal of a Walled Garden intercept, respectively. (Joint Stip. ¶ 3.)

During document discovery, Frontier produced data from its DMCA database. (*Id.* ¶ 11.) The earliest produced Reports table data dates back to September 2, 2019; the earliest produced Notifications table data dates to October 27, 2012[12]; and the earliest WG_Intercept table data is from August 11, 2017. (*Id.*) Reports in the DMCA Database which predate September 2, 2019 were automatically purged by Frontier's automated systems on or before March 2, 2020. (*Id.* ¶ 12.) Frontier created the programs which periodically clear out its data, and modifies those programs from time to time. (*Id.*)

The DMCA script also writes information about the processing of Notices into a text file known as a system log ("syslog"). (*Id.* ¶ 16.) The DMCA script creates an entry in the syslog when it "processes a particular Notice and encounters a particular threshold or encounters a particular error," whereupon it writes a message in the syslog indicating that it encountered the threshold/error when processing that Notice. (*Id.*) The kinds of errors the script makes a note of include, but are not limited to, "(i) when it cannot parse the XML contained in a Notice; or (ii) if the owner field for the IP address identified in the Notice cannot be populated." (*Id.*) If Frontier did not receive a Notice, the Notice was not processed by Frontier's system and no error was recorded in the syslog files. (Levan Decl. ¶ 16.) Levan testified that, when he reviewed the

[12] Levan testified that the Notifications table data dates back to October 12, 2012, not October 27. (Levan Decl. ¶ 13(b).)

litigation hold circulated within Frontier on January 25, 2021, preserving syslog files did not occur to him. (*Id*. ¶ 18.) On or about March 23, 2021, however, "prompted by some event or inquiry to believe that it might be useful to retain the syslog files for purposes of this litigation," Levan disabled the automatic deletion of syslogs and extended the retention period from 45 days to an indefinite period.[13] (*Id.* ¶ 19; Joint Stip. ¶ 17.) Frontier retains and has produced syslogs from February 6, 2021 to March 16, 2024. (Levan Decl. ¶19.)

The DMCA script also creates daily "backtrace files" for debugging purposes when the script encounters errors that cause it to terminate. (Joint Stip. ¶ 18.) Frontier retains and has produced these backtrace files from May 13, 2022 onward. (*Id.*)

In addition to the above, Frontier maintains audio recordings of customer calls, a fraction of which it started to transcribe in October of 2022 by using an artificial intelligence tool. (Response at 6–7.) Until August of 2024, Frontier automatically deleted these transcripts after 90 days. (Vosburgh Decl. ¶ 13.) In August of 2024, Kevin Vosburgh, the Director of Frontier's Data Analysis division, became aware of this litigation and instructed his colleagues to extend the preservation period to 120 days. (*Id.*) After his deposition on November 7, 2024, he instructed his team to preserve all transcripts going forward from that date "while issues in the case play out." (*Id.* ¶ 14.) The underlying audio recordings of the deleted transcripts still exist, as well as notes of calls made by customer service representatives; it is not clear from the briefing what was produced to plaintiffs. (Response at 7.)

2. Timeline of Notices, Cease-and-Desist, Proofs of Claims

On September 19, 2016, Frontier received a demand letter from non-party RightsCorp, Inc. concerning alleged copyright infringement. (Motion at 20.) Frontier responded on October

[13] Technically, the retention period is set to 50 years. (Nov. 12 Levan Dep. Tr. 373:6–17.)

13, 2016 denying liability, but placed a hold on emails of its then-in-house counsel Cecilia Stiber. (*Id.* at 21.) This hold was a "strategic legal hold," not a "litigation hold," meaning that it was implemented for business reasons. (Mauri Decl. ¶¶ 2, 6–7.) This strategic hold on Stiber's emails was lifted on September 12, 2017. (*Id.* ¶ 8.) At this time, Frontier did not change its policy of deleting Reports data older than six months. (Motion at 21; Joint Stip. ¶ 6.) RightsCorp never sued Frontier. (Response at 4.)

The MCCs began sending notices of infringement to Frontier as early as March 12, 2016. They filed 149,483 notices to Frontier from October 14, 2016 through September 1, 2019. (Culpepper Decl. ¶ 2.)

Counsel to the MCCs sent a cease-and-desist letter ("Cease and Desist") to Frontier on March 10, 2020, which Frontier received that day. (Motion at 8; ECF Doc. # 2302 at 7–14 (Cease and Desist).) The Cease and Desist noted that counsel for the MCCs had filed a lawsuit in Hawaii against a separate entity for copyright infringement, and that the MCCs had sent "over 191,300 notices per the Digital Millenium Copyright Action [sic]" to Frontier (including hundreds related to specific IP addresses). (ECF Doc. # 2302 at 8–10.) Counsel for the MCCs also alleged in the letter that Frontier failed to qualify for DMCA safe harbors because it, per his analysis, lacked a policy for dealing with repeat infringers, and alleged that Frontier is liable for the alleged copyright infringements. (*Id.* at 9–10.) While the Cease and Desist noted that the MCCs wished to "resolve this issue outside of litigation if possible," it also stated that the MCCs would "consider any and all legal action necessary to protect their valuable intellectual property rights under federal and state law," and expressly reserved all rights. (*Id.* at 10.) The Cease and

Desist identified a handful of specific IP addresses which the MCCs allege were connected to copyright infringement.[14]

On March 31, 2020, Frontier's in-house counsel, Paul Garcia, replied to the MCCs' demand letter. (*See* ECF Doc. # 2302 at 24.) Garcia set out Frontier's view that it was "confident that no court would find Frontier liable for direct or contributory copyright infringement," picked apart the legal reasoning in the Cease and Desist in some detail, and stated, "Frontier and its operating subsidiaries would vigorously defend against claims against them, and would seek any and all available remedies—including without limitation their reasonable attorneys' fees—all of which are expressly reserved." (*Id.* at 24–26.)

On April 14, 2020, Frontier filed for bankruptcy. (ECF Doc. # 1.)

On May 26, 2020, Frontier's in-house counsel sent an email noting that "some . . . accounts . . . fell through cracks because of the programming situation" discussed internally at Frontier (details are not known to the Court at this time). (Ex. M-5 to the Motion at 5.) Garcia asked, "Are we able to identify these customers, or do we need to know the time frame of the violations to do so?," and identified five problematic IP addresses, including three of those which the MCCs had specified in their Cease and Desist.[15] (*Id*.) Another Frontier employee was able to pull account information for those five IP addresses, indicating, according to the MCCs, that Frontier still had detailed account information relating to those five IP addresses as of May 27, 2020. (Motion at 14.) Later, during the course of this litigation, the MCCs served Frontier with a request for identification of those customers assigned to the three IP addresses which the MCCs identified in their Cease and Desist and for which Frontier had possessed information as

[14] Specifically, 47.146.148.100; 32.211.168.134; 50.47.111.3; 50.45.234.126; 32.208.214.132; 32.209.75.93; 32.210.96.25; 32.210.1 14.34; 32.210.215.115; and 32.211.168.134. (Motion at 12.)

[15] Specifically, 32.211.168.134, 32.210.96.25, and 32.210.215.115. (*Id.*)

of May of 2020, but Frontier was not able to produce IP address assignment records from 2016 through 2021 for those addresses; the MCCs consider this to be proof that Frontier destroyed evidence which they should have known, on account of the Cease and Desist, would be relevant to the litigation. (*Id.* at 15.) The MCCs point out that, at the time of the Cease and Desist, Frontier's practice was to preserve IP address assignment records for 24 months, so in the spring of 2020, it could have preserved records dating back to 2018—but did not. (*Id*.)

A number of copyright-holders filed proofs of claim against Frontier on June 8, 2020, reflecting pre-petition claims against Frontier. (Culpepper Decl. ¶ 44.) More filed through June 1, 2021. (Motion at 15.)

Counsel for the MCCs began communicating with Frontier's counsel during its bankruptcy by, at latest, September 28, 2020, seeking a stipulation lifting the automatic stay for the MCCs' copyright claims.[16] (Culpepper Decl. ¶ 48.) Frontier replied on October 14, 2020, stating it would not so stipulate. (*Id.* ¶ 49.) On December 4, 2020, Frontier proposed disallowing the MCCs' claims in the bankruptcy proceeding but permitting the MCCs to pursue their claims in state or federal court after Frontier emerged from bankruptcy. (*Id.* ¶ 52; *see also* Exhibit M-9 to the Motion.) On December 14, Frontier subsequently suggested to the MCCs that, if they wished to resolve their claims in bankruptcy court, the parties would "need to conduct an evidentiary hearing before the Bankruptcy Court to adjudicate the extent (if any) of the Debtors' liability," and that the parties would have to "meet and confer regarding scheduling and the scope of discovery," and asked for opposing counsel's schedule. (Exhibit M-9 to the Motion.) Both sides met and conferred on December 28. (Culpepper Decl. ¶ 54.) Counsel for the MCCs sent a follow-up email to Frontier on December 28, 2020, specifying that the MCCs

[16] Despite this, Frontier frames the MCCs' stance as "shift[ing] direction towards litigation" only in December 2020. (Response at 5.)

would seek IP address information in discovery. (Exhibit M-9 to the Motion.) On January 8, 2021, Frontier's outside counsel emailed the MCCs, proposing topics for discovery and expressly contemplating litigation before this Court. (Culpepper Decl. ¶56.) The two sides met and conferred regarding a discovery schedule on January 14, 2021. (*Id*. ¶ 57.) On January 18, counsel for the MCCs sent to Frontier's counsel a letter detailing information requested by Frontier during the meet-and-confer, including copyright certificates and an Excel sheet listing more than 200,000 Notices and corresponding IP addresses and dates sent to Frontier from April of 2016 through December of 2020. (*Id.* ¶ 58.) Frontier maintains that it cannot find "any record" of this list of 200,000 IP addresses; the MCCs contest this. (Response at 6 n.5; Supplemental Motion.)

On January 25, 2021, Frontier issued a litigation hold memorandum directing members of its DMCA team—the group in charge of reviewing information about subscriber accounts and deciding whether to terminate their Internet access—to preserve all documents "potentially relevant" to the MCCs' claims, as well as all records related to each of the MCCs' works at issue (listed in an exhibit to the litigation hold), "all customer information related to the IP addresses purported to have engaged in copyright infringement, including without limitation" a set including those identified by the MCCs and listed in another exhibit to the litigation hold[17]; all communications with "the above-identified customers" (presumably those linked to the identified IP addresses) that relate to any claims of copyright violation; documents related to Frontier's DMCA compliance; and some other categories of information. (Exhibit 5 to the Response.) Upon receiving the litigation hold, Levan ensured that the contents of the DMCA Database existing at that time were preserved. (Response at 6; Levan Decl. ¶¶ 9, 10.) However,

[17] This exhibit—Exhibit B—seems to have vanished. Philippe Levan was one of the recipients of the January 25, 2021 litigation hold; he testified that he never received Exhibit B. (Levan Decl. ¶ 8.).

Frontier did not think that syslogs fell within the scope of the discovery items flagged by the MCCs, and since it believed them to be "largely irrelevant to Frontier's DMCA database and script," the litigation hold memorandum did not include a requirement to preserve syslogs. (Response at 6.) Syslogs were not preserved until Levan decided, apparently of his own accord, to maintain them in March of 2021. (*Id.*) Frontier also did not preserve the data in the RADIUS database until around March of 2021, at which time Levan instructed a colleague to preserve old RADIUS tables going forward. (*Id.*) Six months' worth of RADIUS data, dating from January to June 2019, was preserved; Frontier claims that this preservation effort was soon forgotten, however, and RADIUS data was not further preserved (outside of the usual retention periods) until June of 2024. According to Frontier, this means that it preserved "all of the IP address information available in RADIUS related to Notices Frontier received and processed, either in the preserved RADIUS tables or within the information captured in the DMCA Database, from January 1, 2019, onwards, except for the small window of July–August 2019." (*Id.* at 6 n.6.) (This does not account for the failure to begin preserving syslogs on January 25, 2021—the day when the first litigation hold was circulated—or earlier.)

All of the activity by Frontier in preserving records leaves a substantial gap—few records dating back to the date for the statute of limitations (April 13, 2017) were retained.

In May 2023, Frontier produced to the plaintiffs the entire DMCA database, which included over 1.3 million Reports dating back to September 2, 2019, over 6 million Notifications dating back to October 12, 2012, and over 159,000 records in the WG_Intercept table dating back to August 17, 2017. (Response at 8.) Frontier frames it thus: the DMCA database produced to plaintiffs "identifies by name over 11,000 subscribers whose accounts were subject to MCC Notices going back to 2016." (*Id.* at 18.)

In November 2023, the MCCs served their first document requests, seeking, among other files, the identities of Frontier subscribers assigned to particular IP addresses in 959 instances of alleged infringement stretching from 2016 through 2020 (i.e., 959 dates/times of alleged infringement, each associated with a specific IP address). (Response at 7.) (Neither party explains whether the 959 instances all involved unique IP addresses, or if IP addresses were repeated in the set of 959 instances.) The MCCs obtained an order from this Court (ECF Doc. # 2264, the "Cable Act Order") requiring Frontier to identify subscribers associated with 911 IP address/time stamp pairs. (*Id.*) Frontier then queried its DMCA Database and identified 93 subscribers. (*Id*.) For some of the remaining IP address/time stamp pairs, Frontier's databases never contained information sufficient to identify the subscribers; Levan explained that, since the subscriber information data in the DMCA database came from Frontier's RADIUS database, this means that the RADIUS database also lacked the necessary identifying information. (Levan Decl. ¶ 45.) For others, Frontier was not able to identify accounts because data in the Reports table older than September 2, 2019 had been purged automatically as of March 2020. (Response at 7.) In November 2024, Frontier found the six months' worth of RADIUS data tables dating back to 2019, queried that data, and identified an additional 198 unique subscribers along with their IP address assignment histories, corresponding to 430 of the 959 instances requested by the MCCs. (Levan Decl. ¶¶ 46–48.)

Also in November 2023, the MCCs requested "written notes of verbal communications with customers subject to [N]otices." (Motion at 24.) Frontier did not produce call transcripts to the MCCs at that time, only producing them in October 2024; it is not clear from the briefing why production was delayed. (*Id.* at 6–7.) Of the transcripts produced from over 1,000 calls (Response at 16 n.14.), the MCCs managed to identify one call with a customer who had

previously been terminated for repeat infringement, but who seems to have been reinstated as a customer (Motion at 24).

The MCCs sent subpoenas to the subscribers Frontier had identified pursuant to the Cable Act Order. (Appendix C to the Response.) According to Frontier, most recipients ignored the subpoenas, ten denied having relevant documents and many of the ten denied infringement, and seven settled with the MCCs by signing a declaration drafted by the MCCs' counsel in exchange for a release from liability. (Response at 8.) One of the two subscribers whom the MCC deposed "largely recanted the declaration MCCs' counsel had drafted for him." (*Id*.)

3. Greg Hartman's Emails

Greg Hartman was a member of Frontier's DMCA team. He left Frontier on November 8, 2019, and was not an agreed-upon custodian in this litigation. (Response at 1, 15.) By March 10, 2020, Frontier had deleted his emails. (*Id.* at 10–11.) During his tenure at Frontier, Hartman generated reports of repeat infringers and intended to identify an individual flagged for copyright infringement who seemed to be a Frontier company employee. (Motion at 24.) This is significant because Frontier, per the MCCs, does not have a safe harbor defense against liability resulting from its own employees' infringement. (*Id.* at 25.) Hartman testified that he never identified a specific employee and did not recall creating any documents relating to this issue. (Hartman Decl. ¶ 9.)

Frontier has a record of the preservation of Hartman's hard drive and no record of its destruction, but has not been able to locate the hard drive. (Motion at 20.) Frontier has produced emails sent to and from Hartman to the extent that they have appeared in custodians' inboxes and hit on search terms. (Response at 15–16.)

II. LEGAL STANDARD

Spoliation is defined as "the destruction or significant alteration of evidence, or the failure to preserve property for another's use as evidence in pending or reasonably foreseeable litigation." *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 216 (S.D.N.Y. 2003) (internal citation omitted). Federal Rule of Bankruptcy Procedure 7037 incorporates FRCP 37. FRCP 37(e) deals with the spoliation of evidence stored in electronic or digital form:

> (e) Failure to preserve electronically stored information. If electronically stored information that should have been preserved in the anticipation or conduct of litigation is lost because a party failed to take reasonable steps to preserve it, and it cannot be restored or replaced through additional discovery, the court:
>
> (1) upon finding prejudice to another party from loss of the information, may order measures no greater than necessary to cure the prejudice; or
>
> (2) only upon finding that the party acted with the intent to deprive another party of the information's use in the litigation may:
>
> (A) presume that the lost information was unfavorable to the party;
>
> (B) instruct the jury that it may or must presume the information was unfavorable to the party; or
>
> (C) dismiss the action or enter a default judgment.

FED. R CIV. P. 37(e).

Rule 37(e) requires "a three-part inquiry":

> The first is to decide if the rule applies at all—that is, if a party failed to take "reasonable steps" to preserve electronically stored information "that should have been preserved in the anticipation or conduct of litigation." FED. R. CIV. P. 37(e). If so, then the second step is to decide if there has been "prejudice to another party from loss of the information," in which case the Court "may order measures no greater than necessary to cure the prejudice." FED. R. CIV. P. 37(e)(1). Lastly, the third step to consider—regardless of prejudice to any other party—is whether the destroying party "acted with the intent to deprive another party of the information's use in the litigation," in which event a court may consider whether to impose the most severe of measures such as mandatory presumptions or instructions that the lost information was unfavorable or the entry of default judgment.

Morgan Art Found. Ltd. v. McKenzie, No. 18 CV 4438 ATBCM, 2020 WL 5836438, at *16–17 (S.D.N.Y. Sept. 30, 2020) (internal citation omitted).

Under Rule 37(e), prior to ordering sanctions, courts must also find that the destroyed evidence "cannot be restored or replaced through additional discovery." FED. R. CIV. P. 37(e). Additionally, courts must find either that the loss of information prejudiced another party or "that the party acted with the intent to deprive another party of the information's use in the litigation." FED. R. CIV. P. 37(E)(1)–(2). "An evaluation of prejudice from the loss of information necessarily includes an evaluation of the information's importance in the litigation." FED. R. CIV. P. 37(e) advisory committee's note to 2015 amendment.

The sanctions permitted under subsection (e)(1), available upon a finding that the spoliation caused "prejudice to another party," must be limited to "measures no greater than necessary to cure the prejudice." FED. R. CIV. P. 37(e)(1). Thus, if the only prejudice to the movant "lies in the extra time and expense that have been necessary to obtain relevant discovery from third parties," *Lokai Holdings LLC v. Twin Tiger USA LLC*, No. 15-CV-9363 (ALC) (DF), 2018 WL 1512055, at *12 (S.D.N.Y. Mar. 12, 2018), monetary sanctions may be sufficient. Other sanctions permissible under subsection (e)(1) include more "serious measures," such as "forbidding the party that failed to preserve information from putting on certain evidence, permitting the parties to present evidence and argument to the jury regarding the loss of information, or giving the jury instructions to assist in its evaluation of such evidence or argument." FED. R. CIV. P. 37(e)(1) advisory committee's note to 2015 amendment. *See also Karsch v. Blink Health Ltd.*, No. 17-CV-3880-VMB-CM, 2019 WL 2708125, at *27–28 (S.D.N.Y. June 20, 2019) (allowing, as Rule 37(e)(1) sanction, the movant to present evidence of spoliation and the potential relevance of the spoliated evidence to the factfinder); *Lokai*, 2018 WL 1512055, at *17 (precluding, pursuant to Rule 37(e)(1), the spoliating party from offering evidence at trial as to the content of spoliated evidence, "including any testimony suggesting that

such [evidence] would have supported any elements of their defenses or counterclaims"); *Medcenter Holdings Inc. v. Web MD Health Corp*., 692 F. Supp. 3d 81, 101 (S.D.N.Y. 2023), *amended on reconsideration*, 734 F. Supp. 3d 303 (S.D.N.Y. 2024) (precluding spoliating party from presenting evidence "as to the nature or value of the" spoliated evidence, even absent evidence of intent to deprive the other side of evidence). In determining the extent of the prejudice, "[i]n many cases . . . it would be unfair to require affirmative proof as to whether the evidence would have been advantageous to the movant as a predicate to subsection (e)(1) sanctions . . . it is well-established that, as between a negligent party and an innocent party, the former has no right to retain the fruits of their misconduct." *Karsch*, 2019 WL 2708125, at *20 (cleaned up). Courts have found a showing of prejudice sufficient where "the existing evidence plausibly suggests that the spoliated ESI could support the moving party's case." *Id*. (cleaned up, collecting cases).

However, to obtain the "particularly harsh" sanctions listed in subsection (e)(2)—including adverse inference instructions and terminating sanctions—the court must first find that the party to be sanctioned acted with the "intent to deprive another party of the information's use in the litigation." *Lokai*, 2018 WL 1512055, at *8 (internal citation omitted). "Absent a showing of 'intent to deprive another party of the information's use in the litigation,' the sanctions enumerated under subsection (2) of Rule 37(e) are not available." *Id.* at *7; *see also Mazzei v. The Money Store*, 656 Fed. App'x 558, 560 (2d Cir. 2016) (concluding that an adverse inference can be granted only upon finding that party acted with intent to deprive). Negligence or even gross negligence are insufficient to trigger an adverse inference. *Lokai*, 2018 WL 1512055, at *8.

The "party seeking spoliation sanctions"—here, the MCCs—"has the burden of establishing the elements of a spoliation claim by a preponderance of the evidence." *Dilworth v. Goldberg*, 3 F. Supp. 3d 198, 200 (S.D.N.Y. 2014); *see also McIntosh v. United States*, No. 14-CV-7889 (KMK), 2016 WL 1274585, at *33 (S.D.N.Y. March 31, 2016).

III. DISCUSSION

A. Reasonable Foreseeability of Litigation

The Second Circuit has determined that "[t]he obligation to preserve evidence arises when the party has notice that the evidence is relevant to litigation or when a party should have known that the evidence may be relevant to future litigation." *Fujitsu Ltd. v. Fed. Express Corp*., 247 F.3d 423, 436 (2d Cir. 2001). "[A]nyone who anticipates being a party or is a party to a lawsuit must not destroy unique, relevant evidence that might be useful to an adversary." *Zubulake*, 220 F.R.D. at 217. In this context, "'relevance' means relevance for purposes of discovery, which is 'an extremely broad concept.'" *Orbit One Commc'ns, Inc. v. Numerex Corp*., 271 F.R.D. 429, 436 (S.D.N.Y. 2010) (internal citation omitted). Therefore, "[w]hile a litigant is under no duty to keep or retain every document in its possession[,] it is under a duty to preserve what it knows, or reasonably should know, is relevant in the action, is reasonably calculated to lead to the discovery of admissible evidence, is reasonably likely to be requested during discovery and/or is the subject of a pending discovery request." *Zubulake*, 220 F.R.D. at 217 (cleaned up). The duty to preserve arises when litigation is "reasonably foreseeable." *Off. Comm. of Unsecured Creditors of Exeter Holdings, Ltd. v. Haltman*, No. CV 13-5475 JS AKT, 2015 WL 5027899, at *8 (E.D.N.Y. Aug. 25, 2015), *report and recommendation adopted*, No. 13-CV-5475(JS)(ARL), 2016 WL 128154 (E.D.N.Y. Jan. 12, 2016) (collecting cases).

"A party's duty to preserve is based on a two-part inquiry: (1) when did the duty to preserve arise, and (2) what evidence was the party obligated to preserve?" *Lokai*, 2018 WL 1512055, at *9. "The obligation to preserve evidence arises 'most commonly when suit has already been filed, providing the party responsible for the destruction with express notice, but also on occasion in other circumstances, as for example when a party should have known that the evidence may be relevant to future litigation.'" *Leidig v. Buzzfeed, Inc*., No. 16 CIV. 542 (VM) (GWG), 2017 WL 6512353, at *8 (S.D.N.Y. Dec. 19, 2017) (quoting *Kronisch v. United States*, 150 F.3d 112, 126–27 (2d Cir. 1998)). Thus, where, as here, a party sends a demand letter, the court must determine "whether a reasonable party in the same factual circumstances would have reasonably foreseen litigation." *World Trade Centers Ass'n, Inc. v. Port Auth. of New York & New Jersey*, No. 15-CV-7411 (LTS) (RWL), 2018 WL 1989616, at *4 (S.D.N.Y. Apr. 2, 2018), *adopted by* 2018 WL 1989556 (Apr. 25, 2018) (internal citation omitted); *see also, e.g.*, *Karsch*, 2019 WL 2708125, at *18 (holding that a duty to preserve began when plaintiff sent a "demand letter . . . threatening litigation").

Crucially, the obligation to preserve only applies "to documents that a party knew or 'should have known' were relevant to future litigation." *Leidig*, 2017 WL 6512353, at *9 (quoting *Fujitsu*, 247 F.3d at 436). The Second Circuit has made "clear that relevant in [the context of a spoliation motion] means something more than sufficiently probative to satisfy Rule 401 of the Federal Rules of Evidence." *Residential Funding Corp. v. DeGeorge Financial Corp*., 306 F.3d at 108–09 (internal quotations omitted). "It is not enough for the innocent party to show that the evidence would have been responsive to a document request. The innocent party must also show that the evidence would have been helpful in proving its claims or defenses—i.e., that the innocent party is prejudiced without that evidence. Proof of relevance

does not necessarily equal proof of prejudice." *Best Payphones, Inc. v. City of New York*, No. 1-CV-3924 (JG) (VMS), 2016 WL 792396, at *6 (E.D.N.Y. Feb. 26, 2016), *aff'd as modified sub nom. Best Payphones, Inc. v. Dobrin*, 409 F. Supp. 3d 130 (E.D.N.Y. 2018). "[T]he absence of prejudice can be shown by demonstrating . . . that the other parties were able to obtain the same evidence from another source," *R.F.M.A.S., Inc. v. So*, 271 F.R.D. 13, 25 (S.D.N.Y. 2010), *adopted by R.F.M.A.S., Inc. v. So*, 271 F.R.D. 55 (S.D.N.Y. 2010), or that the "evidence would not support the innocent party's claims or defenses," *Pension Comm. of Univ. of Montreal Pension Plan v. Banc of Am. Sec*., 685 F. Supp. 2d 456, 469 (S.D.N.Y. 2010), *abrogated on other grounds by Chin v. Port Auth. of New York & New Jersey*, 685 F.3d 135 (2d Cir. 2012).

1. RADIUS Database, Syslogs

The MCCs argue that Frontier should have reasonably foreseen litigation as far back as 2016, when RightsCorp sent a demand letter concerning unrelated violations to Frontier. (Motion at 20–21, Reply at 10–11.) This is incorrect, as RightsCorp's letter concerned claims entirely unrelated to this litigation. *See Leidig*, 2017 WL 6512353, at *9. The MCCs' argument that Frontier's duty to preserve evidence kicked in on November 12, 2019 fails for the same reason: Frontier convincingly explains that the litigation hold imposed at the time on the emails of Josh Elmore and Philippe Levan was for an unrelated matter.

However, the Court finds that the evidence presently before it does not allow it to determine when the duty to preserve evidence was triggered with respect to the RADIUS database, the syslogs, and the call transcripts.

It is true that numerous cases in this Circuit have found that, in the copyright context, a cease-and-desist letter triggers a duty to preserve, especially when the content of that cease-and-desist clearly indicated that litigation was on the table. *See CBF Industria de Gusa S/A v. AMCI*

Holdings, Inc., No. 13-CV-2581-PKC-JLC, 2021 WL 4190628, at *14 (S.D.N.Y. Aug. 18, 2021) (holding that a demand letter triggered duty to preserve when it "specifically put Defendants on notice that they could expect a lawsuit regarding alleged fraudulent transfer and alter ego claims relevant to the pending arbitration"); *Lokai*, 2018 WL 1512055, at *10 (finding that a cease-and-desist triggered the duty to preserve when it contained an "unmistakable threat of litigation": the letter communicated to defendants the plaintiff's "position that Defendants had violated [the plaintiff's] intellectual property rights . . . enclosing a copy of the trademark certificate, and indicated that [plaintiff] would consider taking 'legal action' if Defendants did not provide a 'satisfactory response' to the Cease-and-Desist Letter within seven days of receipt"); *Usenet.com*, 608 F. Supp. 2d at 430 (ruling that a cease-and-desist letter regarding alleged copyright infringement sufficient to trigger duty to preserve: "Where copyright infringement is alleged, and a cease and desist letter issues, such a letter triggers the duty to preserve evidence, even prior to the filing of litigation.") (internal citation omitted); *Regulatory Fundamental Group v. Governance Risk Management*, No. 13cv2493 (KBF), 2014 WL 3844796, at *6, *13 (S.D.N.Y. 2014) (finding that a cease-and-desist letter threatening to "seek legal recourse" if recipients failed to comply with demands contained in the letter was arguably sufficient to trigger obligation to preserve documents). Moreover, the MCCs' March 10, 2020 Cease and Desist explicitly accuses Frontier's subscribers of infringing on the MCCs' copyrights, blames Frontier for failing to terminate repeat infringers, alleges that Frontier fails to qualify for the DMCA safe harbor, and states that Frontier is liable for copyright infringement. It sets out specific potential remedies the MCCs' counsel believes are available to his clients, including an injunction and damages. While the letter suggests that the MCCs "would like to resolve this issue outside of litigation if possible," it made such an offer to settle contingent on Frontier taking significant

action to cut off allegedly infringing subscribers and to pay "a portion of my clients' [the MCCs'] damages," and threatened to take "any and all legal action necessary to protect" the MCCs' intellectual property rights. Frontier's response is also telling: in delving into the merits of the MCCs' allegation and promising to "vigorously defend against [the MCCs'] claims," Frontier seems to have conceded that they very well could wind up in a court battle with the MCCs. Frontier's protestations that this Cease and Desist was like "multiple previous demand letters concerning its DMCA processes, none of which had resulted in litigation," and that it therefore did not put Frontier on notice of litigation, fail in the face of Mr. Garcia's response to the MCCs and the clear language of the Cease and Desist.[18] (Response at 10–11 n.11.) The Court finds that the Cease and Desist does contain an "unmistakable threat of litigation." Frontier acted at its own risk ignoring the Cease and Desist. Frontier cannot disregard its obligation to preserve records because litigation or bankruptcy claims had not previously been filed. This leaves the question of what records should have been retained starting on March 10, 2020.[19]

At least one other exchange should have tipped off Frontier to the likelihood of litigation with the MCCs before January 2021 (i.e., before Frontier circulated its first litigation hold internally). The exchanges Frontier had with the MCCs' counsel in December 2020 gave Frontier plenty of notice of impending litigation. Starting on December 14, Frontier's counsel and Mr. Culpepper emailed about discovery that would need to be taken. Frontier obviously was aware by December 2020 that the MCCs would seek document discovery, including discovery

[18] The cases Frontier cites to support its argument that cease-and-desist letters do not uniformly trigger the duty to preserve evidence are not binding on this Court, nor do they contradict this holding.

[19] This also does not address the preservation of documents that may be necessary for Frontier to assert an affirmative defense under the DMCA, for which Frontier carries the burden of proof. Such issues are beyond the scope of this Opinion.

specifically concerning a litany of IP addresses. Frontier's argument that the MCCs at that time "did not indicate that they would seek IP address histories but only subscriber names" falls flat in the face of Frontier's own system for identifying subscribers accused of copyright infringement: in order to find a subscriber name associated with an IP address linked to alleged infringement on a particular date (the information provided in a Notice), Frontier would need to go through its IP address histories (the RADIUS database). One cannot have one—the subscriber name—without the other—the IP address history. Despite these exchanges and meet-and-confers, Frontier waited for over a month, until January 25, 2021, to circulate its first litigation hold internally. Frontier entirely fails to explain this delay.

What is not clear at present is whether Frontier should have anticipated preserving the *system logs and RADIUS database specifically*, either in March or December 2020. There is no evidence in the record before the Court at this time that adequately shows that Frontier knew or should have known *in 2020* to preserve these sources of information. The claimants may present additional evidence and argument at trial to attempt to prove this point.

However, the absolute latest point at which Frontier should have started preserving RADIUS data, at least, was on January 25, 2021, when it issued its first litigation hold. As the MCCs point out, the litigation hold required recipients to preserve "all customer information related to the IP addresses purported to have engaged in copyright infringement." (Supplemental Motion at 2.) By its plain terms, this language covers IP address assignment history. And at least one of the litigation hold's recipients should have understood that—Philippe Levan. In an email exchange with other Frontier employees, he explained in early February 2020 that some IP addresses are in dynamically-assigned pools and that, to identify a subscriber tied to an IP address at which infringement allegedly occurred, he would need to know "a specific time period

to identify the customer without ambiguity": in other words, he would need to look at that IP address's assignment history to determine the appropriate customer information for a given Notice (i.e., for a given instance of alleged infringement). And IP address assignment history, as he testified in his deposition, is in the RADIUS database. (June 6 Levan Dep. Tr. 223:19–24.) Levan therefore should have begun preserving RADIUS data on January 25, 2021 at the very latest—and possibly as early as March 10, 2020.

2. Records Tables

As for the Records data, Frontier stated in its Response that it produced to the MCCs "all the data that was present in the database as of their March 10, 2020 demand letter and through the date of collection in 2024," and the "only evidence lost from that [DMCA] database was purged before March 2, 2020, by the automated operation of Frontier's systems." (Response at 22.) The MCCs do not deny this. Given the present record, the Court finds that the earliest that Frontier could have anticipated this litigation is March 10, 2020, and that Frontier preserved all Records tables which it was obligated to keep. The Court therefore **DENIES** the MCCs' Motion with regards to the Records tables.

3. Call Transcripts

It is not at present clear to the Court when any obligation to preserve call transcripts may have kicked in, as neither side has sufficiently explained whether the MCCs' November 2023 request for "written notes of verbal communications with customers subject to [N]otices" covered transcripts, nor is it clear why, if so, Frontier did not produce transcripts at that time and waited until October 2024. The question of when the obligation to preserve the transcripts will have to be determined at trial. (As Frontier points out, call transcripts did not exist at the time of the Cease and Desist, nor in December 2020.)

4. Greg Hartman's Emails

The Court finds that Frontier was under no obligation to preserve or produce more of Greg Hartman's emails than it already has. Hartman left the company in November 2019, and Frontier had deleted his emails by March 2020 pursuant to what appears to be their routine data management practice. It also appears that Frontier has expended reasonable efforts in trying to obtain those documents of Hartman's which may still exist and be responsive to the plaintiffs' document requests. The Court **DENIES** the MCCs' Motion insofar as it pertains to Hartman's documents.

B. Prejudice

The extent of the prejudice which the MCCs suffered due to the deletion of the RADIUS database, syslogs, and call transcripts is also not clear from the incomplete record presently before the Court. The MCCs argue that without these records, they will have a harder time with both (1) proving direct infringement, due to their inability to identify a large number of subscribers associated with IP addresses specified in Notices during and predating 2019; and (2) attacking Frontier's anticipated repeat infringer policy defense, given the absence of identifying information for many of Frontier's allegedly infringing subscribers in light of Frontier's scrubbing of its RADIUS database, and the relative lack of evidence showing that Frontier reinstated repeat infringers.

The prejudicial effect on the MCCs' ability to prove direct infringement is not clear, since the Court does not at present know the scope of evidence and expert testimony the MCCs plan to present on this point at trial. As noted above, it does not appear to be the case that the MCCs or RCCs have to pursue each and every alleged infringer to show instances of direct infringement; circumstantial evidence, rather than evidence from possibly thousands of

subscribers, may be sufficient. The Court therefore cannot at present determine whether or to what extent Frontier's deletion of RADIUS data hampered the MCCs. Frontier did provide—albeit belatedly—105 subscriber identifications on December 9, 2024, after querying those RADIUS tables from 2019 which it did preserve. (Reply at 4.) It appears to the Court that, with this production, Frontier has produced all those subscriber identities relevant to this litigation which the MCCs requested and which Frontier still possesses at this time. The MCCs point out that, as "deadlines have passed, [they] cannot obtain favorable evidence"—i.e., evidence of direct infringement—"from these 105 subscribers." (*Id.*) The MCCs and RCCs have not been bashful about asking for more discovery when they think the Frontier has not been responsive to outstanding document requests. As this case approaches trial in May 2025, discovery is over, except perhaps for trial subpoenas.

Regarding the difficulty of attacking Frontier's section 512(i) affirmative defense without syslogs, call transcripts, and the RADIUS database: again, without a fuller understanding of other sources of evidence concerning Frontier's repeat infringer policy and its implementation, the Court is unable to determine the extent of the prejudice (if any) incurred by the plaintiffs. It is clear that Frontier had repeat infringers—hence the existence of the Notifications and WG_Intercept tables. It also appears likely that, without IP address assignment histories, it could be difficult for plaintiffs to prove, for example, that Frontier did not implement its policy consistently or in a reasonable manner, or otherwise allowed too many repeat infringers to remain customers of Frontier. If this is the case, Frontier will not be permitted to benefit from its destruction of evidence. However, without knowing what other sources of evidence exist, this Court simply cannot prejudge the extent of the prejudice to the plaintiffs, nor can it determine at

present the prejudicial effect (if any) of destroying a given type of evidence. The parties will have to argue this point at trial.

C. Frontier's Mental State

Again, the Court finds that it does not have sufficient evidence to determine the mental state with which Frontier deleted evidence. The MCCs' argument that Frontier's shortening of the RADIUS retention period from 24 months to 18 during the pendency of this litigation was persuasively rebuffed by Frontier, as it appears that Frontier needed to make this change to keep its system operational. The MCCs have otherwise generally failed to advance evidence in support of their argument that Frontier acted with an intent to deprive plaintiffs of relevant evidence. Given that the RCCs will presumably argue this point at trial, the Court abstains from ruling on it at present.

IV. CONCLUSION

In sum, the Court will not, at present, impose Rule 37(e) sanctions upon Frontier, but may do so at trial after further evidence and argument. The Court **DENIES** the MCCs' Motion as applied to Greg Hartman's emails and the Records tables, but it permits the MCCs to argue spoliation with regards to the RADIUS database, call transcripts, and syslogs at trial, along with the RCCs. The Court also **ORDERS** the MCCs, if they wish to seek additional evidence from the pool of 105 newly-identified Frontier subscribers accused of direct infringement, to submit a letter brief to the Court explaining their need for this discovery.

Dated: January 23, 2025
New York, New York

Martin Glenn

MARTIN GLENN
Chief United States Bankruptcy Judge